# COMPUTING $S$-INTEGRAL POINTS ON ELLIPTIC CURVES OF RANK AT LEAST 3 (Analytic Number Theory : Arithmetic Properties of Transcendental Functions and their Applications)

AUTHOR(S):

Hirata-Kohno, Noriko; Lality-Kovacs, Tunde

CITATION:

Hirata-Kohno, Noriko ...[et al]. COMPUTING $S$-INTEGRAL POINTS ON ELLIPTIC CURVES OF RANK AT LEAST 3 (Analytic Number Theory : Arithmetic Properties of Transcendental Functions and their Applications). 数理解析研究所講究録 2014, 1898: 92-102

ISSUE DATE:

2014-05

URL:

http://hdl.handle.net/2433/195893

数理解析研究所講究録
第1898巻 2014年 92-102



# COMPUTING $S$-INTEGRAL POINTS ON ELLIPTIC CURVES OF RANK AT LEAST 3

N. HIRATA-KOHNO AND T. KOVÁCS

ABSTRACT. We give all the S-integral points of elliptic curves via considering linear forms in elliptic logarithms both the complex and the $p$-adic case. We apply a lower bound for linear forms in $p$-adic elliptic logarithms in arbitrary number of terms.

## 1. INTRODUCTION

It is well-known Siegel [20] proved in 1929 that the number of the integral points on an elliptic curve $E$ over an algebraic number field $\mathbb{K}$ is finite and Mahler [17] generalized this result to the $S$-integral points where $S$ is a finite set of places defined over $\mathbb{K}$. Relying upon the group structure of $E(\mathbb{Q})$ and properties of ordinary elliptic logarithms, a different method for proving the finiteness of ordinary integral points was proposed by Lang [14], Masser [18] and Zagier [27]. Using the explicit lower bound for linear forms in ordinary elliptic logarithms by David [4], the argument by Lang, Masser and Zagier could be transformed into an algorithm for computing the integer points on elliptic curves which was done by Gebel, Pethő, Zimmer [6], Stroeker, Tzanakis [24], Smart [22]. However, the approach depends on an unproved lower bound for linear forms in $p$-adic elliptic logarithms. In 1996, Rémond and Urfels proved such a bound for linear forms in two terms. Using this bound and following Smart's line of thought, Gebel, Pethő and Zimmer in [7], [8], found all $S$-integral points on Mordell's curves $y^2 = x^3 + k$, with $|k| \leq 10^4$ and such that the rank of the curve $< 3$. In [9], Gebel, Herrmann, Pethő and Zimmer could overcome the absence of an explicit lower bound for linear forms in $p$-adic elliptic logarithms by using the completely explicit upper bound for the $S$-integral solutions of elliptic equations established by Hajdu and Herendi [10]. They determined the $S$-integral solutions of several elliptic curves of various ranks up to 8 and compared their results with earlier estimates. As of rank at most 2 elliptic curves, their method gives only a larger upper bound for the $S$-integral points than using the estimate of Rémond and Urfels. This suggests that the existence of a similar bound to that of Rémond and Urfels for higher rank curves would lead to a similar lessening in the size of the upper bound of the $S$-integral points. This is important in particular if the rank of the elliptic curve is large, as then already a small improvement of the final bound can considerably shrink the region of possible solutions, and hence the final search can be done much faster.

2000 *Mathematics Subject Classification.* Primary 11G05, secondary 11Y50.

*Key words and phrases.* Elliptic curves, S-integral points, linear forms in elliptic logarithms, LLL-algorithm.

Research supported in part by the OTKA grant 100339 and by JSPS, Funding Program for Next Generation World-Leading Researchers (NEXT Program), GR087.

We show here an algorithm to find all $S$-integral points of elliptic curves of rank greater than 2. As it was pointed out in Smart [23], the previous methods could be extended to do so, however the theory of lower bounds for linear forms in $p$-adic elliptic logarithms was not developed enough. As a new lower bound for linear forms in $p$-adic elliptic logarithms has been proved [11], we could extend the very efficient method using ordinary and $p$-adic elliptic logarithms first established by Gebel, Pethő and Zimmer in [7], [8], to the case of elliptic curves of arbitrary rank. In Section 2 we give the necessary notation and describe our method in detail. In Section 3 we give an example. We include larger prime numbers in the set $S$ which is a new feature compared to the previously solved elliptic equations.

## 2. Bounding the $S$-integral points of elliptic curves

We describe the method of finding the $S$-integral points on elliptic curves in a most detailed way. We shall refer to the papers [7], [8], [9], [22]. Let $E$ be a given elliptic curve defined by the equation

$$E: \quad y^2 = x^3 + ax + b := q(x).$$

Here $a, b \in \mathbb{Z}$ and the discriminant of $q(x)$, i.e. $4a^3 + 27b^2$ is non-zero. By Mordell's theorem, the group $E(\mathbb{Q})$ of rational points on $E$ is finitely generated. More precisely,

$$E(\mathbb{Q}) \cong E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r,$$

where $E_{tors}(\mathbb{Q})$ is the torsion group, and $r$ is the rank of $E(\mathbb{Q})$. Let $P_1, \ldots, P_r$ denote a Mordell-Weil basis of $E(\mathbb{Q})$. Then each rational point $P \in E(\mathbb{Q})$ has a unique representation of the form

$$P = P_0 + n_1 P_1 + \ldots + n_r P_r, \tag{1}$$

where $P_0 \in E_{tors}(\mathbb{Q})$ is a torsion point and $n_i \in \mathbb{Z}$ $(i = 1, \ldots, r)$.

We fix an arbitrary finite set $S$ of places of $\mathbb{Q}$ (including the infinite one) to be

$$S := \{p_1, \ldots, p_{s-1}, \infty\}.$$

Let $E(\mathbb{Z}_S)$ denote the set of $S$-integral points of $E(\mathbb{Q})$, i.e.

$$E(\mathbb{Z}_S) = \{P = (x, y) \in E(\mathbb{Q}) | H_S(P) \leq 1\},$$

where

$$H_S(P) = \prod_{q \notin S} \max\{1, |x|_q\}$$

with $|x|_q$ being the normalized multiplicative absolute value of $\mathbb{Q}$ corresponding to the place $q$. Put $N := \max_{1 \leq i \leq r} |n_i|_\infty$. If one searches for the set $E(\mathbb{Z}_S)$ then first an upper bound for $N$ has to be found and then this bound has to be gradually decreased to a size where the actual points can already be identified by an exhaustive search. To get the final bound $N_{final}$ for $N$, the LLL-algorithm is applied. In the following subsections we explain in detail how one proceeds.

2.1. **Height.** The multiplicative height of a rational point $P = (x, y) \in E(\mathbb{Q})$ is defined as the following product over all primes $p$ of $\mathbb{Q}$ (including $p = \infty$):

$$H(P) := \prod_p \max\{1, |x|_p\}.$$

Here we define the ordinary additive height as

$$h(P) := \frac{1}{2} \log H(P) \tag{2}$$

and the Néron-Tate height is

$$\hat{h}(P) := \frac{1}{2} \lim_{n \to \infty} \frac{h(2^n P)}{2^{2n}}.$$

It is well-known (see for example [3]), that for all $P = (x, y) \in E(\mathbb{Q})$ we have

$$\hat{h}(P) - h(P) \leq c_1,$$

where $c_1$ is an explicitly computable positive constant depending only on the parameters of the curve. (Later $c_2$, $c_3$, etc. will be also explicitly computable positive constants depending only on the parameters of the curve and sometimes on the chosen Mordell-Weil basis of the curve.) Furthermore, since $\hat{h}$ is a positive semidefinite quadratic form on $E(\mathbb{R})$, we obtain the lower estimate

$$\hat{h}(P) \geq \lambda_1 N^2,$$

where $\lambda_1 > 0$ is the smallest eigenvalue of the height-pairing matrix with respect to the basis $P_1, \ldots, P_r$ of $E(\mathbb{Q})$. On combining the latter two inequalities, we get the estimate

$$h(P) \geq \lambda_1 N^2 - c_1. \tag{3}$$

Let now $P = (x, y) \in E(\mathbb{Q})$ be an $S$-integral point and choose $p \in S$ such that

$$|x|_p = \max\{|x|_{p_1}, \ldots, |x|_{p_{s-1}}, |x|_\infty\}. \tag{4}$$

Then we conclude that

$$H(P) \leq |x|_p^s, \quad \text{with } s := \sharp S,$$

hence that

$$h(P) \leq \frac{s}{2} \log |x|_p. \tag{5}$$

Combining (3) and (5) yields the upper bound

$$\frac{1}{|x|_p^{1/2}} \leq c_2 \exp(-c_3 N^2) \tag{6}$$

with

$$c_2 = \exp\left(\tfrac{c_1}{s}\right), \quad c_3 = \tfrac{\lambda_1}{s}.$$

2.2. **Elliptic logarithms.** A lower bound for $|x|_p^{-1/2}$ can be obtained by estimating linear forms in elliptic logarithms. Here two cases are to be distinguished, the complex case and the $p$-adic case.

2.2.1. *Case 1:* $p = \infty \in S$. We shall use the Weierstrass-parametrization of our elliptic curve $E$. There exists a lattice $\Omega \subseteq \mathbb{C}$ such that the group of complex points is

$$E(\mathbb{C}) \cong \mathbb{C}/\Omega,$$

where $\Omega = \langle \omega_1, \omega_2 \rangle$ is generated by the two fundamental periods $\omega_1$ and $\omega_2$, where $\omega_1$ is real and $\omega_2$ is complex. We put $\tau = \omega_2/\omega_1$ and assume without loss of generality that $\Im\tau > 0$. The above isomorphism is defined by Weierstrass' $\wp$-function with respect to $\Omega$ and its derivative $\wp'$ according to the assignment

$$P = (\wp(u), \wp'(u)) \leftarrow u \bmod \Omega,$$

so that the coordinates of an integral point $P = (x, y) \in E(\mathbb{Q})$ are given by

$$x = \wp(u), \ y = \wp'(u).$$

The elliptic logarithm of $P$ is then (see e.g. [27])

$$u = u(P) \equiv \int_x^\infty \frac{dt}{\sqrt{t^3 + at + b}} \pmod{\Omega}.$$

Also, for later use define

$$\phi(P) := u(P)/\omega_1.$$

Actually, we have

$$u = u(P) \equiv n_1 u_1 + n_r u_r + u_{r+1} (\text{mod } \Omega),$$

where $u_i \in \mathbb{R}$ are the (complex) elliptic logarithm of the generating points $P_i$ of $E(\mathbb{Q})$. Equivalently, we have

$$\phi(P) \equiv n_1 \phi(P_1) + n_r \phi(P_r) + \phi(P_{r+1}) (\text{mod } 1).$$

Hence an integer $n_0$ exists such that

$$\phi(P) = n_0 + n_1 \phi(P_1) + n_r \phi(P_r) + \phi(P_{r+1}),$$

so that assuming all $\phi$-values belong to $[0, 1)$,

$$|n_0| < rN + 1.$$

Let $t$ be the order of the torsion point $P_{r+1}$. Then $t\phi(P_{r+1}) \equiv \phi(\mathcal{O}) \equiv 0 \pmod 1$, and hence $\phi(P_{r+1}) = s/t$, for some non-negative integer $s < t$. Thus,

$$\phi(P) = \left(n_0 + \frac{s}{t}\right) + n_1 \phi(P_1) + \ldots + n_r \phi(P_r).$$

Now let

$$\Lambda := u(P) = \left(n_0 + \frac{s}{t}\right) \omega_1 + n_1 u_1 + \ldots + n_r u_r. \tag{7}$$

In 1995, David [4] computed a lower bound for linear forms in complex elliptic logarithms of shape (7). His bound involves the following quantities:

$$g := |E_{tors}(\mathbb{Q})|, \quad c_4 := 2.9 \cdot 10^{6r+6} \cdot 4^{2r^2} (r+1)^{2r^2+9r+12.3},$$

where $r$ is the rank of the curve,

$$h := \log\left(\max\{4|a \cdot j_2|_\infty, 4|b \cdot j_2|_\infty, |j_1|_\infty, |j_2|_\infty\}\right),$$

where $j := j_1/j_2$ is the $j$-invariant of the curve, and some numbers $V_i \in \mathbb{R}$ satisfying

$$\log V_i \geq \max\left\{\hat{h}(P_i), h, \tfrac{3\pi|u_i|^2}{\omega_1^2 \cdot \Im(\tau)}\right\}, \quad (i = 1, \ldots, r).$$

Using David's result, the desired lower bound for $|x|_\infty^{-1/2}$ is given in the following lemma.

**Lemma 2.1.** *With the above notation we have*

(8)

$$\frac{\omega_1}{g\sqrt{8}} \exp\left(-c_4 h^{r+1}\left(\log\left(\frac{r+1}{2}gN\right)+1\right)\left(\log\log\left(\frac{r+1}{2}gN\right)+1\right)^{r+1} \cdot \prod_{i=1}^{r} \log V_i\right) \leq \frac{1}{|x|_\infty^{1/2}}.$$

Comparing the inequalities (6) and (8), we can derive an upper bound for $N$ in the complex case.

2.2.2. *Case 2: $p = p_i \in S$ (for some $i \in \mathbb{N}$ such that $1 \leq i \leq s-1$).* Up to now there were only partial results in this case due to the lack of a $p$-adic analogue of David's lower bound for linear forms of arbitrary number of terms. Indeed, a lower bound for linear forms in two terms was proved by Rémond and Urfels [19] in 1996. Recently, a generalization of this result to arbitrary number of terms was given by the first author. Using the bound, we can get an analogue of (8). We explain in detail how one proceeds in the $p$-adic case.

Let $\mathbb{Q}_p$ be the $p$-adic completion of $\mathbb{Q}$ and $\mathbb{Z}_p$ its ring of $p$-adic integers. Denote by

$$E_0(\mathbb{Q}_p) := \{P \in E(\mathbb{Q}_p) | \tilde{P} \text{ is non-singular}\},$$

as well as by

$$E_1(\mathbb{Q}_p) := \{P \in E(\mathbb{Q}_p) | \tilde{P} = \tilde{\mathcal{O}}\}$$

the kernel of the reduction map modulo $p$, where $E$ is regarded as a curve over $\mathbb{Q}_p$ and $\tilde{P}, \tilde{\mathcal{O}}$ are the reduced points $P, \mathcal{O}$ modulo $p$. It is known that if $E$ is minimal at $p$, then $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is finite and equal to the Tamagawa number $c_q$.

Designate by $\mathcal{E}(p\mathbb{Z}_p)$ the formal group associated to $E$ (see e.g. [21]). We consider the isomorphism

$$\mathcal{E}(p\mathbb{Z}_p) \to E_1(\mathbb{Q}_p), \quad z \mapsto \begin{cases} 0, & \text{if } z = 0, \\ (\frac{z}{w(z)}, -\frac{1}{w(z)}), & \text{if } z \neq 0, \end{cases}$$

where

$$z = -\frac{x}{y}, \quad w(z) = -\frac{1}{y}.$$

The equation for $w = w(z)$ inferred from the long Weierstrass equation for $E(\mathbb{Q})$ (i.e. of the shape $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$) becomes

$$w = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3 = f(z, w).$$

A recursive procedure based on this equation (see [21]) leads to the power series

$$w = z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1a_2 + a_3)z^6 \\ + (a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4)z^7 + \ldots \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]].$$

This is the unique power series in $z$ satisfying the relation

$$w(z) = f(z, w(z)).$$

From it we also get the Laurent series for $x$ and $y$, respectively.

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1a_3)z^2 - \ldots, \\ y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1a_3)z + \ldots. \tag{9}$$

The invariant differential has the expansion

$$w(z) = (1 + a_1 z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + a_3)z^3 \\ + (a_1^4 + 3a_1^2a_2 + 6a_1a_3 + a_2^2 + 2a_4)z^4 + \ldots)dz.$$

Note that in these expansions the coefficients of the powers of $z$ each have the same weight depending on the exponent of $z$.

The $p$-adic elliptic logarithm is now the image under the homomorphism to the additive group $\hat{G}_a$ (over the completion $\mathbb{C}_p$ of the algebraic closure of $\mathbb{Q}_p$) defined as follows:

$$\psi_p : E_1(\mathbb{Q}_p) \to \hat{G}_a, \quad P = (x, y) \mapsto \psi_p(P) = \int w(z) = z + \frac{d_2}{2}z^2 + \frac{d_3}{3}z^3 + \ldots.$$

In particular, the $p$-adic logarithm $\psi_p$ has the properties

$$\psi_p(P + Q) = \psi_p(P) + \psi_p(Q)$$

and

$$|\psi_p(P)|_p = |z|_p = \left|-\frac{x}{y}\right|_p.$$

Now let $\tilde{E}$ be the reduced curve $E$ modulo $p$ and denote by $\mathcal{N}_p = \sharp\tilde{E}(\mathbb{F}_p)$ the number of rational points on $\tilde{E}/(\mathbb{F}_p)$ and let $c_p$ denote the Tamagawa number with respect to $p$. With the order $g$ of the torsion subgroup of $E$ introduced earlier, we define

$$m := m_p = lcm(g, c_p \cdot \mathcal{N}_p).$$

Then, we have from the Lutz filtration of $E$, see e.g. [16],

$$mP_i =: P_i' \in E_1(\mathbb{Q}_p) \quad (i = 1, \ldots, r)$$

for the generating points $P_i$ of $E(\mathbb{Q})$ and

$$mP_0 = \mathcal{O}$$

for the torsion points $P_0 \in E_{tors}(\mathbb{Q})$.

The representation (1) of an $S$-integral point $P = (x, y) \in E(\mathbb{Q})$ gives rise to the representation

$$P' = n_1'P_1 + \ldots + n_r'P_r = n_1P_1' + \ldots + n_rP_r', \quad (n_i' := mn_i \in \mathbb{Z}) \tag{10}$$

of its $m$-multiple $P' = (x', y') = mP \in E_1(\mathbb{Q}_p)$. In analogy to (9), we have the Laurent series

$$x' = \frac{z'}{w(z')} = \frac{1}{z'^2} - \frac{a_1}{z'} - a_2 - a_3 z' - (a_4 + a_1 a_3) z'^2 - \ldots,$$

and this expansion entails the estimate

$$|x'|_p \leq \frac{1}{|z'|_p^2} = \frac{1}{|t'|_p^2}, \tag{11}$$

where we use the abbreviating notation $t' := \psi_p(P')$ for the $p$-adic elliptic logarithm of $P'$.

Combining inequalities (6) and (11) and observing that $|x'|_p \geq |x|_p$, we obtain the

$$|t'|_p \leq \frac{1}{|x'|_p^{1/2}} \leq \frac{1}{|x|_p^{1/2}} \leq c_2 \exp(-c_3 N^2) \tag{12}$$

upper bound for the $p$-adic elliptic logarithm $t' = \psi(P')$ of the point $P' = (x', y') = mP$. Therefore, what we need is a lower estimate for the $p$-value of the $p$-adic elliptic logarithm $t'$ of $P'$.

From the additive property of the $p$-adic elliptic logarithm and (10), we have the relation

$$t' = n_1' t_1 + \ldots + n_r' t_r = n_1 t_1' + \ldots + n_r t_r' =: \Lambda$$

between the elliptic logarithms $t' = \psi_p(P')$ of $P'$, $t_i = \psi_p(P_i)$ of the generating points $P_i$ and $t_i' = \psi_p(P_i')$ of their $m$-multiples $P_i' = mP_i \in E(\mathbb{Q})$. Let

$$\begin{gathered}
c_5 := 2^{4r^2+3r} \cdot (r+1)^{2r^2+9r+4}, \\
h' := \log \max(1, |a|_\infty, |b|_\infty), \\
a_i := \max(1, \hat{h}(P_i'), h') \quad (1 \leq i \leq k), \\
\beta := \max(1, 2h(n_1), \ldots, 2h(n_r)), \\
\rho := p^{-\lambda_p} \quad \text{for } \lambda_p := \begin{cases} \frac{1}{p-1} & \text{if } p > 2, \\ 3 & \text{if } p = 2, \end{cases} \\
\sigma := \rho / \max(|t_1'|_p, \ldots, |t_r'|_p), \\
\delta := \max(1, (\log \sigma)^{-1}), \\
\gamma := \max(1, h', \log a_1, \ldots, \log a_r, \log \delta).
\end{gathered}$$

Then we have the following result.

**Lemma 2.2.** *With the above notation, whenever we have $\Lambda \neq 0$, we obtain*

$$|\Lambda|_p > \exp(-c_5 \cdot \delta^{2r+2} \cdot \max(\beta, \gamma) \cdot \gamma^{r+1} \cdot a_1 \cdots a_r \cdot \log \sigma).$$

**Remark 2.1.** *The dependance on the prime $p$ appears in the definition of $\sigma$.*

**Remark 2.2.** *Note that the definition of additive height in* [11] *differs by a factor* 2 *from* (2), *therefore this difference also occurs in the definition of $\beta$ comparing to the corresponding parameter* $\log B$ *of* [11].

For any sufficiently large $N$, the inequality of Lemma 2.2 can be turned into

$$\exp(-c_6 \cdot \log N) \leq |t'|_p, \tag{13}$$

with $c_6 = c_5 \cdot \delta^{2r+2} \cdot \gamma^{r+1} \cdot a_1 \cdots a_r \cdot \log \sigma$.

**Remark 2.3.** *Note that in contrast to the lower bound of David and that of Rémond and Urfels, estimation* (13) *does not contain the factor* $\log\log N$.

Comparing the inequalities (12) and (13), we can derive an upper bound for $N$ in the $p$-adic case, as well.

2.3. **LLL-reduction.** Comparing the inequalities (6) and (8), we get

$$c_3N^2 \leq c_4h^{r+1}\prod_{i=1}^{r}\log V_i\left(\log\left(\frac{r+1}{2}gN\right)+1\right)\left(\log\log\left(\frac{r+1}{2}gN\right)+1\right)^{r+1}+$$
$$+\log c_2-\log\left(\frac{\omega_1}{g\sqrt{8}}\right)$$

in the complex case and comparing the inequalities (12) and (13), we get

$$c_3N^2 \leq c_6\log N+\log c_2$$

in the $p$-adic case. In both cases, for sufficiently large $N$, the left hand side exceeds the right hand side. Hence we obtain an initial upper bound $N \leq N_{0,p}$ for all $p \in S$. However, this initial bound is too large to determine all $S$-integer solutions of the given equation. Therefore we have to reduce it somehow. Actually, we use the $LLL$-algorithm to do that. Again, we have to distinguish between the complex and the $p$-adic case. As we do not know which $p$ satisfies our assumption (4), we need to consider all possibilities. For the application of the $LLL$-algorithm, we refer to the paper of Smart [22].

After carrying out the $LLL$ reduction as many times as it improves the upper bound for $N$, in case of all $p \in S$, we have to choose the worst of them to be $N_{final}$. Then we have to check the $(2N_{final}+1)^r$ possible points whose coordinates satisfy $|n_i| \leq N_{final}$, $(i=1,\ldots,r)$, whether they are $S$-integral points.

## 3. Example

We illustrate the efficiency of our method through an example.

**Theorem 3.1.** *All* $\{101,103,107,\infty\}$*-integral solutions of the equation* $y^2=x^3-203472x+18487440$ *are contained in Table 1.*

Table 1: $S$-integral points $P=(x,y)=\left(\frac{\xi}{\zeta^2},\frac{\eta}{\zeta^3}\right)=\Sigma_{i=1}^{5}n_iP_i$ on $E: y^2=x^3-203472xA18487440$ for $S=\{101,103,107,\infty\}$

| $\xi$ | $\eta$ | $\zeta$ | $\xi$ | $\eta$ | $\zeta$ |
|---|---|---|---|---|---|
| 950904 | 1076191164 | 103 | 72 | 2052 | 1 |
| −1960272 | 7321044924 | 101 | 468 | 5076 | 1 |
| 1348776 | 1566425412 | 1 | −216 | 7236 | 1 |
| −351 | 6831 | 1 | 53856 | 12497868 | 1 |
| 720 | 15660 | 1 | 432 | 3348 | 1 |
| 17452 | 2304748 | 1 | −279 | 7317 | 1 |
| 7092 | 596052 | 1 | 157212 | 62334252 | 1 |

Table 1 – continued from previous page

| $\xi$ | $\eta$ | $\zeta$ | $\xi$ | $\eta$ | $\zeta$ |
|---|---|---|---|---|---|
| 2448 | 119124 | 1 | 14176 | 1686988 | 1 |
| 81 | 1593 | 1 | 4 | 4204 | 1 |
| −468 | 3348 | 1 | 8388 | 767124 | 1 |
| 496 | 6292 | 1 | 748 | 16876 | 1 |
| 31169169 | 172016429031 | 103 | −36 | 5076 | 1 |
| −488 | 1252 | 1 | 4320 | 282420 | 1 |
| 1944 | 83484 | 1 | 396 | 108 | 1 |
| 372941316 | 7202126555028 | 1 | −5554328 | 2128421132 | 107 |
| 45548136 | 307401450948 | 1 | −5618484 | 484446852 | 107 |
| 55656 | 13129668 | 1 | −1063136 | 6724595116 | 103 |
| 13689 | 1600749 | 1 | 520 | 7300 | 1 |
| 28429684 | 149496531724 | 103 | 433 | 3401 | 1 |
| 1526904 | 1886763996 | 1 | 1188 | 38124 | 1 |
| 90108 | 27048276 | 1 | 36 | 3348 | 1 |
| 7272 | 618948 | 1 | 22392 | 3350052 | 1 |
| 3897 | 241677 | 1 | 163872 | 66336948 | 1 |
| 8958384 | 22533294204 | 107 | −195480 | 4874042700 | 101 |
| −432 | 5076 | 1 | −351936 | 5199314724 | 101 |
| −72 | 5724 | 1 | −423 | 5373 | 1 |
| 2916 | 155628 | 1 | 576 | 9612 | 1 |
| −1427220 | 7931134980 | 107 | 3204 | 179604 | 1 |
| −180 | 7020 | 1 | 88 | 1124 | 1 |
| 1404 | 50004 | 1 | 4869657 | 5656377123 | 101 |

**Remark 3.1.** *For every $S$-integral point $P = (x, y)$ on $E$, of course $-P = (x, -y)$ is an $S$-integral point, too. Because of the large number of $S$-integral point pairs, we listed only one from each pair in Table 1, in particular the one with positive second coordinate.*

Proof of Theorem 3.1.

Let $E$ denote the curve

$$E: \quad y^2 = x^3 - 203472x + 18487440$$

and set

$$S = \{101, 103, 107, \infty\}.$$

The rank of $E$ is 5 and a basis of the Mordell-Weil group is

$$P_1 = (36, 3348), \quad P_2 = (-36, 5076), \quad P_3 = (432, 3348),$$

$$P_4 = (-216, 7236), \quad P_5 = (468, 5076).$$

First we compute the basic data of our curve. We find that the torsion subgroup is trivial, therefore (1) reads as

$$P = n_1 P_1 + \ldots + n_5 P_5.$$

TABLE 2. The data computed to get an initial upper bound for $N$ in the $p$-adic case for $p \in \{101, 103, 107\}$.

| $p$ | 101 | 103 | 107 |
|---|---|---|---|
| $\lambda_p$ | 1/100 | 1/102 | 1/106 |
| $\sigma$ | $101^{99/100}$ | $103^{101/102}$ | $107^{105/106}$ |
| $\delta$ | 1 | 1 | 1 |
| $c_6$ | $1.394984 \cdot 10^{141}$ | $9.607104 \cdot 10^{141}$ | $4.352003 \cdot 10^{141}$ |

TABLE 3. The new bound for $N$ in each case of $p$ after the $i$th step of reduction is $N_{i,p}$.

| $i$ | $N_{i,101}$ | $N_{i,103}$ | $N_{i,107}$ | $N_{i,\infty}$ |
|---|---|---|---|---|
| 1 | 93 | 93 | 93 | 93 |
| 2 | 18 | 17 | 17 | 17 |
| 3 | 14 | 15 | 15 | 15 |

As usual, let $N = \max(|n_1|, \ldots |n_5|)$. We compute the Tamagawa numbers $c_{101} = c_{103} = c_{107} = 1$ and

$$\mathcal{N}_{101} = 108, \quad \mathcal{N}_{103} = 104, \quad \mathcal{N}_{107} = 96.$$

Using these data we can compute the numbers $m_p$ and obtain that $m_p = \mathcal{N}_p$ for $p \in \{101, 103, 107\}$.

Next we derive an upper bound of shape (6). We find that $c_1 = 3.575681\ldots$, $\lambda_1 = 0.464930\ldots$ and $s = 4$. Therefore we arrive at the estimate

$$\frac{1}{|x|_p^{1/2}} \leq 2.444694 \cdot \exp(-0.11623263 \cdot N^2).$$

Now we need to compute a lower bound for each value of $p$. For $p = \infty$, we get

$$\frac{1}{|x|_\infty^{1/2}} \geq 0.09598 \cdot \exp(-2.125933 \cdot 10^{167} \cdot (\log 3N + 1)(\log\log 3N + 1)^6).$$

Comparing the latter two estimates, we get $N \leq N_{0,\infty} = 4.860551 \cdot 10^87$. In the $p$-adic case we compute all data contained in Table 2.

Therefore we get

$$N_{0,101} = 4.4807 \cdot 10^{72}, \quad N_{0,103} = 3.7164 \cdot 10^{72}, \quad N_{0,107} \leq 2.4984 \cdot 10^{92}.$$

The results obtained after each step of LLL-reduction are contained in Table 3. Recall, that we start the reduction with $N_{0,p}$ in the 1st step and then in every further step we repeat the reduction with using the value obtained in the previous step for every $p \in S$. It turns out that 15 cannot be improved further. Therefore we have to check $(2 \cdot 15 + 1)^5 = 31^5$ points whether they are $S$-integral points. We find exactly those ones contained in Table 1.

## REFERENCES

[1] A. BAKER, *Transcendental Number Theory*, Cambridge Univ. Press, (1975).

[2] J. COATES, *An effective p-adic analogue of a theorem of Thue III; the diophantine equation* $y^2 = x^3 + k$, Acta Arith. **74** (1970), 425–435.

[3] J. E. CREMONA, M. PRICKETT AND S. SIKSEK, *Height Difference Bounds For Elliptic Curves over Number Fields*, J. Number Theory **116** (2006), 42–68.
[4] S. DAVID, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France **62** (1995), 143 pp.
[5] S. DAVID AND N. HIRATA-KOHNO, *Linear Forms in Elliptic Logarithms*, J. für die reine angew. Math. **628**, (2009), 37–89.
[6] J. GEBEL, A. PETHŐ AND H. G. ZIMMER, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.
[7] J. GEBEL, A. PETHŐ AND H. G. ZIMMER, *Computing S-integral points on elliptic curves*, In Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, May 1996 (Ed. H. Cohen), Lect. Notes in Comp. Sci., vol. **1122** (Springer Verlag, 1996), pp. 157–171.
[8] J. GEBEL, A. PETHŐ AND H. G. ZIMMER, *Computing integral points on Mordell's elliptic curves*, Collect. Math. **48** (1997), 115–136.
[9] J. GEBEL, E. HERRMANN, A. PETHŐ AND H. G. ZIMMER, *Computing all S-integral points on elliptic curves*, Math. Proc. Camb. Phil. Soc. **127** (1999), 383–402.
[10] L. HAJDU AND T. HERENDI, *Explicit bounds for the solutions of elliptic equations with rational coefficients*, J. Symbolic Comp. **25** (1998), 361–366.
[11] N. HIRATA-KOHNO, *Linear forms in p-adic elliptic logarithms*, manuscript.
[12] N. HIRATA-KOHNO AND RINA TAKADA, *Linear forms in two elliptic logarithms in the p-adic case*, Kyushu Journal of Mathematics **64**, no. 2, (2010), 239–260.
[13] S. LANG, *Diophantine approximation on toruses*, Amer. J. Math. **86**, (1964), 521–533.
[14] S. LANG, *Elliptic curves: diophantine analysis*, Grundl. Math. Wiss. **231** Springer-Verlag, 1978.
[15] A. K. LENSTRA, H. W. LENSTRA AND L. LOVÁSZ, *Factoring Polynomials with Rational Coefficients*, Math. Ann. **261** (1982), 515–534.
[16] E. LUTZ, *Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques*, J. reine angew. Math. **177** (1937), 238–244.
[17] K. MAHLER, *Über die rationalen Punkte auf Kurven vom Geschlecht Eins*, J. reine angew. Math. **170** (1934), 168–178.
[18] D. W. MASSER, *Linear forms in algebraic points of Abelian functions III*, Proc. London Math. Soc. **33**, (1976), 549–564.
[19] G. RÉMOND AND F. URFELS, *Approximation diophantienne de logarithmes elliptiques p-adiques*, J. Number Theory **57** (1996), 133–169.
[20] C. L. SIEGEL, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. (1929), 1–41.
[21] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106, Springer Verlag, New York, 1986., xii+400 pp.
[22] N. SMART, *S-integral points on elliptic curves*, Math. Proc. Camb. Phil. Soc. **116** (1994), 391–399.
[23] N. SMART, *The algorithmic resolution of Diophantine equations*, London Math. Soc. Student Texts, 41, Cambridge University Press, Cambridge, 1998., xvi+243 pp.
[24] R. J. STROEKER AND N. TZANAKIS, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), 177–196.
[25] R. J. STROEKER AND N. TZANAKIS, *On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an Improvement*, Experimental Math. **8** (1999), 135–149.
[26] KUNRUI YU, *Report on p-adic logarithmic forms*, in: A Panorama of Number Theory, (ed. G. Wüstholz), Cambridge Univ. Press, (2002), 11–25.
[27] D. ZAGIER, *Large integral points on elliptic curves*, Math. Comp. **48** (1987), 425–436.

NIHON UNIVERSITY, COLLEGE OF SCIENCE AND TECHNOLOGY, DEPARTMENT OF MATHEMATICS, SURUGA-DAI, KANDA, CHIYODA, TOKYO 101-8308, JAPAN
*E-mail address*: hirata@math.cst.nihon-u.ac.jp, tkovacs@science.unideb.hu